REMARKS/ARGUMENTS

Favorable reconsideration and allowance of claims 6, 7, 9, 11, 13 and 16 is respectfully requested.

Applicants are submitting with this amendment a copy of the Declaration and Power of Attorney mailed with the above-identified application to the United Patent and Trademark Office (USPTO) on February 08, 2000. Also being submitted with this amendment is a copy of the post card receipt, date stamped by the USPTO February 17, 2000, The post card receipt identifies a one page declaration as being received by the USPTO with the patent application. The copy of the Declaration and Power of Attorney being submitted with this amendment is signed by the inventor's Christian L. Houlberg and Gary S. Borgen and dated February 08, 2000.

MPEP 503 states on page 500-14 that "a postcard receipt which itemizes and properly identifies the paper being filed serves as prima facia evidence of receipt in the USPTO of all the items listed thereon on the date stamped thereon by the USPTO". It is respectfully submitted that the copy of the signed Declaration and Power of Attorney being provided herewith is a sufficient response to the Examiner's request for an oath/declaration signed by both applicants.

The Examiner's objections to the specification are being corrected by this amendment. Specifically, throughout the specification device 24 is labeled KGV-68 as shown in FIG. 1 of the drawings.

The Examiner's objection to the ABSTRACT as exceeding 150 words is also being corrected by this amendment. The ABSTRACT, as amended is substantially less than the maximum of 150 words.

The Examiner's rejection of claims 1-16 under 35 U.S.C. 103(a) as being unpatentable over Borgen and further in view of Maher is respectfully traversed. Claims 1-5, 8, 10, 12, 14 and 15 are being canceled by this amendment so the rejection no longer applies to these claims.

Independent claim 6 is being amended at lines 15-18 to recite the microcontroller (32, FIG. 2) as including an internal EEPROM for storing the crypto key and the associated checkword and a copy of the crypto key and the associated checkword. Claim 8 is being canceled since this limitation was previously recited in claim 8.

Claim 6 is also being amended at lines 37-54 to recite the microcontroller 32 as containing a computer software program for controlling, handling and interpreting the transfer and loading of the crypto key and associated checkword into encryption device

24.

Specifically, claim 6, as amended, recites a computer software program which controls, handles and interprets the transfer of the crypto key and checkword from the key loader 22 to microcontroller 32 and the storage of the crypto key and check word within the EEPROM of microcontroller 32 in the manner depicted in the flow charts of FIGS. 4, 5 and 6. Further, claim 6, now recites the computer software program as controlling, handling and interpreting the loading of the crypto key and checkword into the encryption device 24 as depicted in FIGS. 4 and 7 and the disabling of transmitter 26 during the loading process which is program step 90 of FIG. 7. Amended claim 6 also recites the enabling of transmitter 26 after a successful load of the crypto key and checkword, which is program steps 110 and 114 of FIG. 7.

Borgen teaches a sequencing control circuit 75 connected to an external EPROM 332 and a static RAM 78. The sequencing control circuit 75 is connected to the power control circuit 41 and the RAM interface circuit 76 of Fig. 1A. The external EPROM 332 is also connected to the power control circuit 41 and the RAM interface circuit 76 of Fig. 1A.

Static RAM 78 receives and stores a key word from a loader

276. Sequencing control circuit 75 provides logic signals for controlling read and write operations of static RAM 78, as well as logic signals to allow for transfer or down loading of the key word from the loader 276 to the static RAM 78.

Borgen also teaches sequencing control circuit 75 providing logic signals to interface with an encryption device 286 which allows the key word to be transferred or up loaded from the static RAM 78 to the encryption device 288.

The EEPROM 332 of Borgen provides program instructions which control the sequence of operation within the nonvolatile memory system including static RAM 78. Addressing for the EEPROM 332 is provided by sequencing control circuit 75.

The digital hardware/digital logic circuitry for sequencing control circuit 75 is depicted in detail in FIG. 10. The digital logic circuitry includes ten bit parallel loadable up counter 140, four eight bit latches 180, 206, 208, and 210, control circuit 168, eight by two bit comparator 250, eight-to-one multiplexer circuit 262, Johnson counter 110, eight bit binary counter 230, eleven bit binary counter 182, and four-to-one demultiplexer 334.

Further, the control circuit 168 for sequencing control circuit 75 includes the 26 logic gates illustrated in Figs. 23A-

23F.

The entire non-volatile memory system disclosed in Borgen includes the numerous logic elements illustrated in Figs. 1A (29 logic elements), Fig. 11 (12 logic elements comprising Johnson counter 110), Fig. 13 (20 logic elements comprising counter 140), Fig. 16 (11 logic elements comprising counter 182), Fig. 14 (5 logic elements comprising each of the ten load circuits 162 in Fig. 13), Fig. 17 (8 logic elements comprising each of the latches 180, 206, 208 and 210 of Fig. 10), Fig. 18 (8 logic elements comprising multiplexer circuit 262 of Fig. 10), Fig. 19 (the eight one bit comparator circuits 252 which make up comparator 250 of Fig. 10), Fig. 21 (the logic elements which make up multiplexer circuit 262), Fig. 23A-23F (26 logic elements which make up control circuit 168 of Fig. 10), and Fig. 31 (the logic elements which make up demultiplexer 334 of Fig. 10).

Except for the EEPROM 332 and the static RAM 78, the nonvolatile memory system of Borgen is made of NAND gates, NOR gates, inverters, flip-flops, buffer gates, transmission gates 364-398, transmission gates 340-354 and a binary counter 40 which are basic logic elements used in the design of numerous logic circuits.

The present invention accomplishes the function of Borgen,

but eliminates the need for the extremely complex hard wired logic circuitry of Borgen by replacing the logic circuitry with a microprocessor which generates all the logic signals needed to transfer, store and then load the crypto key and checkword into the encryption device using the computer software program illustrated in FIGS. 4-9, program steps 40-156, and now claimed in amended claim 6. Further, there is no teaching in Borgen of transferring and then loading an associated checkword into the encryption device, although the Examiner asserts this would be obvious in view Maher. Applicants, however, must respectfully disagree since the hard wired logic circuit design of Borgen would necessitate added logic circuitry which more than likely would be as complex or more complex than logic circuitry for the sequencing control circuit 75. It needs to be understood that any change in the function of sequencing control circuit 75 requires a substantial in the hard wired digital logic circuitry of sequencing control circuit 75, a complex electronic design change which applicants respectfully submit is not obvious in view of the teachings of Borgen in view of Maher.

With respect to the claimed microprocessor, the Examiner asserts that Borgen teaches a microprocessor 75. As discussed above sequencing control circuit 75 is a hard wired logic circuit

which comprises NAND and NOR logic gates, flip-flops, i.e. D-type and J-K flip-flops, transmission gates, buffers and inverters. The hard wired logic of sequencing control circuit 75 allows the circuit to perform only one operation or function. Sequencing control circuit 75 was developed using logic equations and truth tables, does not have microprocessor capabilities and is not a general purpose microcontroller which the user programs to accomplish the desired functions.

In addition, the Examiner asserts that Borgen teaches the use of an EEPROM to store the key and associated checkword. As previously discussed, Borgen teaches only the use of an external static RAM 78 to store the key and does even discuss the storing of the checkword. Since static RAM 78 is external to the sequence control circuit 75, additional logic circuitry is required to store the key word in the static RAM 78. Specifically, there is a need for the additional logic circuitry illustrated in Figs. 1A and 7 to implement the key word storage into static RAM 78 and retrieval from static RAM 78. This additional logic circuitry includes NOR gates 79, 84, 88 and 90, inverter 86, dual flip-flop 82, buffers 92, 94, 96 and 100 and their inter connections as well as a power up logic signal generated by the complex logic circuitry of power control circuit

41. By utilizing an internal EEPROM within microprocessor 32 for storage and retrieval of the crypto key and the associated checkword, the need for the complex logic circuitry illustrated in Figs. 1A and 7 is eliminated.

The Examiner asserts that it would be obvious to disable the transmitter during the loading of the key word into the encryption device 288. The Examiner in support of his position states that the possibility of TEMPEST noncompliance would motivate one of ordinary skill in the art to disable the transmitter during the loading process.

Claim 6, as amended, recites the computer software program controlling, handling and interpreting a disabling of the transmitter 26 when the crypto key and associated checkword are loaded into the encryption device 24 and an enabling of the transmitter 26 after a successful load of the crypto key and associated checkword into the encryption device 24.

Since Borgen uses hard wired logic gates to effect the transfer, storage and loading of the key word into encryption device 288, one or ordinary skill in the art would be required to design additional complex hard wired logic circuitry to turn off the transmitter and then turn on the transmitter after the load is complete. This logic circuitry would be as complex if not more

complex than the logic circuits illustrated in FIGS. 1A, 1B and 10, 11, 13, 14, 16, 17, 18, 19, 21 and 23 of Borgen. In addition, the teaching which the Examiner's appears to use as his basis for obviousness "TEMPEST NONCOMPLIANCE" is not mentioned in Borgen. Further, as previously discussed Borgen fails to mention the loading of the associated checkword into the encryption device, which if implemented by Borgen would also require the design of additional complex, hard wired digital logic circuitry. The absence of these teachings lends further support to Applicants' assertion that the invention as recited in amended claim 6 is nonobvious in view of Borgen.

With respect to claim 7, the Examiner asserts that the 8-bit microprocessor recited therein is obvious in view of the sequencing control circuit 75 illustrated in Fig. 1B. As previously discussed, Borgen teaches a hard wired logic circuit that requires multiple digital logic elements including flip-flops, NAND and NOR gates, inverters, buffers and transmission gates to implement a single function, transfer of the key word from loader device 276 to static RAM 78 for storage and then to encryption device 288. Additional functions such as transfer of the associated checkword and turning off the transmitter during the loading of the key word in the encryption device would

require added logic circuitry to the Nonvolatile Memory System of Borgen. Applicants' implemented these additional functions in a very simplistic manner using the recited computer software program and the internal EEPROM and not by adding additional digital logic circuitry.

Claim 9 recites a light emitting diode 36 as displaying a status for the load of the crypto key and associated checkword into the encryption device. Borgen does not provide a teaching or even a suggestion as to this claim limitation. As with each of the other limitations which Borgen fails to disclose or even suggest, this limitation, i.e. adding a status LED for the load would require additional digital logic circuitry to implement the claimed limitation.

Claim 11, as amended, recites a light emitting diode 38 connected to microcontroller 32 as displaying a status for an erase of the crypto key and the associated checkword from the internal EEPROM of microcontroller 32. Again, Borgen fails to suggest a light emitting diode for monitoring the status of the erase of the crypto key and associated checkword from the internal EEPROM. This, in turn, would necessitate additional hardware be added to the Borgen Nonvolatile Memory System to accomplish the results achieved by the computer software program

included in the microprocessor of the present invention.

Claim 13, as amended, recites an 8-bit microcontroller which includes a computer software program for controlling the downloading and transfer of the crypto key and associated checkword from the loader 22, the storage of the crypto key and checkword in the EEPROM of microcontroller 32 and the loading of the crypto key and checkword into the encryption device 24. In addition, the claim recites the transmitter 26 as being disabled during the loading process and being enabled after a successful load of crypto key and checkword into the encryption device 24. The claim also recites light emitting diodes 36 and 38 for providing status of the load and erase functions controlled by the software illustrated in Figs. 4-9.

The above recited limitations are not disclosed, taught or even suggested by the prior art Borgen SIR. The teaching of Borgen is a hard wired logic circuit which is very complex, includes hundreds of logic gates and is capable of performing only one function, the transfer and temporary storage of a key word into the static RAM 78 and the subsequent loading of the key word into the encryption circuit 288. The present invention performs this function and additional functions set forth in the previous paragraph through the use of the computer software

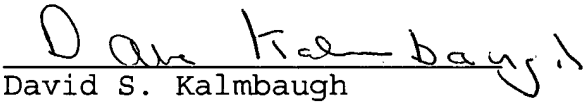
program of Figs. 4-9 and microcontroller 32 with its internal EEPROM. This is definitely not the teaching of Borgen which teaches only a hard wired digital logic circuit capable of performing the single function of transferring the key word from the loader to the static RAM and then to the encryption device.

In view of the foregoing, it is respectfully submitted that amended claims 6 and 13 and the claims dependent therefrom, which are claims 7, 9, 11 and 16, are allowable over the prior art of record. The prior art Borgen SIR and the combination of Borgen and Maher fail to disclose, teach or even suggest an apparatus, such as the apparatus of claims 6 and 13 and the claims dependent therefrom which utilize an 8-bit microcontroller and its computer software program to load the crypto key and associated checkword into the encryption device, disable the transmitter during the loading process, erase the crypto key and checkword after a successful load and control status LEDs which monitor the load and subsequent erasure of the crypto keyword. Without the benefit of the disclosure of Applicants' invention as now claimed and set forth in the above-identified application, the Examiner would be unable to suggest that the invention is obvious, since the prior art fails to provide the required motivation or teaching to suggest to an individual of ordinary skill in the art

to modify the Borgen reference or the combination of Borgen in view of Maher to provide for an efficient, accurate, and reliable apparatus for controlling the loading of crypto key and associated check word into an encryption device that does not compromise national security. And such hindsight is not permissible when trying to assert that an invention is obvious.

In view of the foregoing remarks, it is respectfully submitted that the application is in condition for allowance. The early allowance of claims 6 and 13 and the claims dependent therefrom and the prompt issuance of this case are earnestly solicited.

Respectfully submitted,



David S. Kalmbaugh
Reg. No. 29,234
Tel.: (805) 989-8266

Attachments: (1) Declaration
(2) Post Card Receipt